REMARKS

The applicant acknowledges and appreciates the Examiner's through examination of the application and request re-examination and reconsideration of the application in view of the preceding amendments and following remarks.

The Examiner rejects claims 2 and 18 under 35 U.S.C. 112, second paragraph. The applicants herein amend claims 2 and 18 to address the Examiner's rejection. The applicants respectfully request that the Examiner withdraw the rejection of these claims under 35 U.S.C. 112, second paragraph.

Claims 1-31 stand rejected under 35 U.S.C. 101 because the claims allegedly are directed to non-statutory subject matter.

In a series of well-known cases, the Federal Circuit has clearly stated what subject matter should be considered in determining patentability:

> In State Street, this court, following the Supreme Court's guidance in Diehr, concluded that "[u]npatentable mathematical algorithms are identifiable by showing they are merely abstract ideas constituting disembodied concepts or truths that are not 'useful.' . . . [T]o be patentable an algorithm must be applied in a 'useful' way." Id. at 1373, 47 USPQ2d at 1601. In that case, the claimed data processing system for implementing a financial management structure satisfied the 101 inquiry because it constituted a "practical application of a mathematical algorithm, . . . [by] produc[ing] 'a useful, concrete and tangible result.'"

AT&T Corporation v. Excel Communications, Inc., 50 U.S.P.Q. 2d 1447, 1451 (Fed. Cir. 1999) (emphasis added) (citing *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F3d 1368, 1373, 47 USPQ2d 1596, 1601 (Fed. Cir. 1998), cert. Dnd, 119 S. Ct. 851 (1999).

Thus, contrary to the Examiner's assertion, the advanced encryption standard (AES) engine of the subject invention clearly should be given patentable weight because it produces "a useful, concrete and tangible result." *Id.* A specific useful, concrete and tangible result of the subject invention is that it provides a data encryption engine, which may be implemented in software and/or hardware, for implementing the advanced encryption standard (AES). See independent claim 1 and page 5, lines 2-3 of the subject application. Since the subject invention as claimed by the applicants recites statutory subject matter, applicants respectfully request that the Examiner withdraw this rejection to claims 1-31.

Claims 1, 12-15 and 29 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by US Patent Publication No. 2003/0039355 A1 to McCanny et al.

The invention results from the realization that an advanced encryption standard (AES) engine with real time S-box generation which is faster even than a parallel look-up approach can be achieved with a Galois field multiplier system which in a first mode is responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in $GF^{-1}(2^m)$ and applying an affine over GF(2) transformation to obtain a subbyte transformation; and shift register system for transforming the subbyte transformation to obtain a shift row transformation; the Galois field multiplier system is responsive, in a second mode, to the shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of the first data block.

McCanny et al. relates to a product for generating data encryption/decryption. Fig. 3 of McCanny et al. illustrates a round 24 of the Rijndael algorithm. Round 24 includes a ByteSub transformation 30, a ShiftRow transformation 32, a MixColumn transformation 34 and a Round Key Addition 36. *See* McCanny et al. at page 3, paragraph 41.

The Examiner alleges in the Office Action that McCanny et al. discloses a Galois field multiplier system to obtain a subbyte transformation as claimed by the applicants. McCanny et al. clearly discloses, however, that it uses one or more look-up tables or ROMs to obtain a subbyte transformation:

> A consideration in the design of the apparatus 40 is the memory requirement. The ByteSub module 52 is therefore advantageously implemented as one or more look-up tables (LUTs) or ROMs. This is a faster and more cost-effective (in terms of resources required) implementation than implementing the multiplicative inverse operation and affine transformation in logic.

McCanny et al. at page 4, paragraph 60 (emphasis added). Thus, McCanny et al. clearly fails to disclose the applicants' claimed advanced encryption standard (AES) engine with real time S-box generation that includes a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in GF^1 (2^m) and applying an affine over GF(2) transformation to obtain a subbyte transformation. Rather, McCanny et al. discloses and teaches that it is allegedly preferable to use one or more look-up tables (LUTs) or ROMs.

In contrast to McCanny et al., the subject invention does not require the use of look-up tables to obtain the subbyte transformation. As shown in box 38 of Fig. 3 of the subject patent application, the subbyte transformation can be calculated in two steps. The subbyte transformation is effected using an S-box which first takes the multiplicative inverse in $GF^{-1}(2^8)$ and then applies an affine over GF(2) transformation defined by the matrix expression. *See* the subject application at page 11, line 17 to page 12, line 2. To obtain the multiplicative inverse in $GF^{-1}(2^8)$, Fig. 12 of the subject invention discloses one embodiment of the invention in which a Galois field reciprocal generator 155 having a Galois field multiplier 152 and a second Galois field multiplier 154 for

performing a squaring function. Galois field reciprocal generator 155 generates $1/\beta$ where β is an element of a Galois field, for example, where m = 8, that is $GF(2^8)$: the degree of the field is eight. Alternatively, Figs. 11, 13, 14 and 15 illustrate different configurations of the engine of Fig. 12 to perform different operations. As can be seen, the subject invention does not require the use of look-up tables to obtain the subbyte transformation as does the apparatus of McCanny et al.

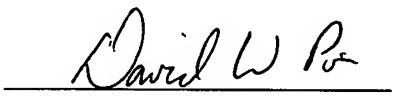
Claim 1 of the subject application recites: "An advanced encryption standard (AES) engine with real time S-box generation comprising: a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in GF^1 (2^m) and applying an affine over GF(2) transformation to obtain a subbyte transformation; and a shift register system for transforming said subbyte transformation to obtain a shift row transformation; said Galois field multiplier system being responsive in a second mode to said shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of said first data block."

As described above, McCanny et al. clearly fails to disclose the applicants' claimed advanced encryption standard (AES) engine with real time S-box generation that includes a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in GF^1 (2^m) and applying an affine over GF(2) transformation to obtain a subbyte transformation. Accordingly, the applicants respectfully request that the Examiner withdraw the rejections of claims 1, 12-15 and 29 under 35 U.S.C. 102(e).

Each of the Examiner's rejections has been addressed or traversed. Accordingly, it is respectfully submitted that the application is in condition for allowance. Early and favorable action is respectfully requested.

If for any reason this Response is found to be incomplete, or if at any time it appears that a telephone conference with counsel would help advance prosecution, please telephone the undersigned or his associates, collect in Waltham, Massachusetts at (781) 890-5678.

Respectfully submitted,



David W. Poirier
Reg. No. 43,007